

ACA 00448
-copy- 3

DOT/FAA/CT-94/51

FAA Technical Center
Atlantic City International Airport,
N.J. 08405

Evaluation of Automated Risk/Vulnerability Assessment Tools

Ed Rao

LIMITED

September 1994

Technical Report

Approved for Federal Aviation Administration use only. This document is exempt from public availability for reasons of civil aviation security. Disclosure of this document outside the Federal Aviation Administration, must have prior approval of the Office of Civil Aviation Security, ACS-1.



U.S. Department of Transportation
Federal Aviation Administration

FEDERAL AVIATION ADMINISTRATION

TECHNICAL CENTER LIBRARY

ATLANTIC CITY INTL. AIRPT, NJ 08405

00014455

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the object of this report.

Technical Report Documentation Page

1. Report No. DOT/FAA/CT-94/51		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle EVALUATION OF AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS				5. Report Date September 1994	
				6. Performing Organization Code ACA-400	
7. Author(s) E. Rao, FAA Technical Center				8. Performing Organization Report No.	
9. Performing Organization Name and Address Department of Transportation Federal Aviation Administration Technical Center Aviation Security Research and Development Service National Airspace System Security Program, ACA-400 Atlantic City International Airport, NJ 08405				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No. DTFA03-93-C-00042	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration Technical Center Atlantic City International Airport, NJ 08405				13. Type of Report and Period Covered Final	
				14. Sponsoring Agency Code ACA-400	
15. Supplementary Notes Report Prepared by: K. Shuck Abacus Technology Corporation 5454 Wisconsin Avenue, Suite 1100; Chevy Chase, MD 20815					
16. Abstract This document provides an evaluation of nineteen automated risk/vulnerability tools for compliance with the FAA's security analysis framework for National Airspace System Facilities. This evaluation will enable FAA management in determining candidate tools ability to fulfill FAA risk/vulnerability assessment needs. The evaluation criteria is based on the major components of the Security Analysis Framework. Evaluation of the tools was based on claims made by tool vendor without any validation or verification of the claims.					
17. Key Words Evaluation Criteria Methodology, Analytical Framework Criteria, Compliance Evaluation, Tool Description, Evaluation Findings, Comparison of Tools Matrix			18. Distribution Statement This document is a record subject to the provisions of 14 CFR 191 es seq. Release of the information contained herein is prohibited without the express written approval of Associate Administrator for Civil Aviation Security or his designee.		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 52	
				22. Price	

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	
1. INTRODUCTION	1
1.1 Objective	1
1.2 Background	1
1.3 Scope	1
2. METHODOLOGY	1
2.1 Criteria Development	2
2.2 Compliance Evaluation	3
3. COMPLIANCE EVALUATION FINDINGS	5
3.1 Analytic System and Software for Evaluating Safeguards and Security	5
3.2 Bayesian Decision Support System	6
3.3 Buddy System	7
3.4 Control-It	7
3.5 CCTA Risk Analysis and Management Methodology	
3.6 Criti-Calc	8
3.7 Expert Auditor/Probe Engine	8
3.8 FRANTIC ABC	9
3.9 IRRAS	9
3.10 International Security Technology/Risk Analysis and Management Program	10
3.11 Los Alamos Vulnerability Assessment	10
3.12 Risk Assessment Matrix	11
3.13 Rank-It	11
3.14 Resource-Allocation Optimization Program for Safeguards	12
3.15 RA/SYS	12
3.16 RiskMan	13
3.17 RiskPac	13
3.18 RiskWatch	14
3.19 Security Assessment Model	14
3.20 Composite Findings	14

TABLE OF CONTENTS (CONTINUED)

		Page
4.	CONCLUSIONS	15
4.1	Analytic System and Software for Evaluating Safeguards and Security	18
4.2	Buddy System	18
4.3	Control-It	18
4.4	CCTA Risk Analysis and Management Methodology	18
4.5	Expert Auditor/Probe Engine	19
4.6	Los Alamos Vulnerability Assessment	19
4.7	RA/SYS	19
4.8	RiskPac	19
4.9	RiskWatch	19
4.10	Security Assessment Model	19
5.	RECOMMENDATIONS	20
6.	REFERENCES	20
7.	GLOSSARY	21
Appendixes		
A -	Security Analysis Framework Components	A-1
B -	Automated Tool Compliance Evaluation	B-1

LIST OF TABLES

		Page
1.	Comparison of Automated Risk/Vulnerability Assessment Tools	16
2.	Comparison of Automated Risk/Vulnerability Assessment Tools (Continued)	17
3.	Automated Risk/Vulnerability Assessment Tool Evaluation	B-2
4.	Automated Risk/Vulnerability Assessment Tool Evaluation (Continued)	B-7

LIST OF ABBREVIATIONS AND ACRONYMS

ALE	Annual Loss Exposure
AALE	Average Annual Loss Exposure
ARTCC	Air Route Traffic Control Center
ASSESS	Analytic System and Software for Evaluating Safeguards and Security
ATCT	Air Traffic Control Tower
BDSS	Bayesian Decision Support System
CCTV	Closed-Circuit Television
CM	Countermeasures
COTS	Commercial Off-The-Shelf
CRAMM	CCTA Risk Analysis and Management Methodology
DOT	Department of Transportation
EA/PE	Expert Auditor/Probe Engine
FAA	Federal Aviation Administration
FIPS PUB	Federal Information Processing Standards Publication
IDS	Intrusion Detection Sensors
IST/RAMP	International Security Technology/Risk Analysis and Management Program
LAVA	Los Alamos Vulnerability Assessment
NAS	National Airspace System
NUREG	Nuclear Regulation
PC	Personal Computer
RAM	Risk Assessment Matrix
RAOPS	Resource-Allocation Optimization Program for Safeguards
ROI	Return On Investment
SAM	Security Assessment Model
TSO	Time Sharing Operations

EXECUTIVE SUMMARY

This document contains an evaluation of 19 available commercial off-the-shelf (COTS) and Government-developed automated risk/vulnerability assessment tools for compliance with the Federal Aviation Administration (FAA) Security Analysis Framework for National Airspace System (NAS) facilities. The objective of this report is to assist FAA management in evaluating the automated tools' ability to fulfill FAA risk/vulnerability assessment needs.

Each automated risk/vulnerability assessment tool was evaluated against criteria derived from individual components of the framework espoused in the FAA Technical Center, Technical Report, DOT/FAA/CT-94/49, Security Analysis Framework: National Airspace System (NAS) Facilities, September 1994. The major components of the Security Analysis Framework are:

- a. Critical assets, risks, and threat likelihoods,
- b. Protection levels, system vulnerabilities, and impacts,
- c. Acceptable protection measure cost plus asset losses, and
- d. Cost-effective countermeasure analysis and design.

A detailed listing of the individual elements of the Security Analysis Framework is provided in Appendix B.

The evaluations of the automated risk/vulnerability assessment tools were conducted with a complete version of the actual tool where possible. These tools were provided without cost by the sponsoring Government agency or commercial vendor for the specific purpose of evaluation. Some evaluations were conducted with a comprehensive demonstration version or limited version of the automated tool when a complete tool was not provided. In a few cases where no version of the automated tool was obtainable, the evaluation was made based solely on claims made in comprehensive product literature provided by the tool's supplier and interviews with supplier personnel. In these instances, the findings were not based on hands-on evaluations and cannot be validated or verified. The detailed results of the evaluation of each automated tool can be found in Appendix B.

For this evaluation, a tool was considered compliant if one of following three conditions were met (or claims were made that they would be met):

- a. The tool performed the process specified in the criterion,
- b. The tool used information or conditions specified in the criterion as input, or
- c. The tool provided information in the area specified by the criterion as output.

Every criterion received one of following four compliance ratings for each automated tool:

- a. Y - the tool meets the criterion (i.e., meet one of the three conditions cited above),
- b. N - the tool does not meet the criterion and cannot be modified to meet it,
- c. M - the tool in the configuration supplied by the manufacturer does not meet the criterion, but can be modified by the user to meet it, or
- d. C - compliance could not be determined.

Ten of the automated risk/vulnerability tools met the majority of the Security Analysis Framework criteria. These 10 automated tools are:

- a. Analytic System and Software for Evaluating Safeguards and Security,
- b. Buddy System,
- c. Control-It,
- d. CCTA Risk Analysis and Management Methodology,
- e. Expert Auditor/Probe Engine,
- f. Los Alamos Vulnerability Assessment,
- g. RA/SYS,
- h. RiskPac,
- i. RiskWatch, and
- j. Security Assessment Model.

None of the above automated risk/vulnerability assessment tools complies with all the Security Analysis Framework criteria without modification. Since the evaluations conducted for this report were performed on some tools using only the claims made in product/marketing literature provided by the tool's sponsor or vendor, it is recommended that an in-depth, hands-on software evaluation be conducted of a select number of automated tools prior to acquisition. The selection of the automated risk/vulnerability tools to be given the

in-depth, hands-on evaluation should be made based on a detailed user requirements analysis and the findings of this report and the following reports:

- a. FAA Technical Center Technical Report, DOT/FAA/CT-94/48, Catalog of Automated Risk/Vulnerability Assessment Tools, July 1994,
- b. FAA Technical Center Technical Report, DOT/FAA/CT-94/49, Security Analysis Framework: National Airspace System (NAS) Facilities, Automated Risk/Vulnerability Assessment Tool, Volumes I-III, September 1994, and
- c. FAA Technical Center Technical Report, DOT/FAA/CT-94/50, Security Requirements Compliance Review: Automated Risk/Vulnerability Assessment Tools, September 1994.

1. INTRODUCTION.

This report provides an evaluation of 19 automated risk/vulnerability assessment tools for compliance with the framework provided in the Federal Aviation Administration (FAA) Technical Center Technical Report, DOT/FAA/CT-94/49, Security Analysis Framework: National Airspace System (NAS) Facilities, Automated Risk/Vulnerability Assessment Tool, September 1994. This evaluation will assist FAA management in measuring the capability of these tools to fulfill FAA risk/vulnerability assessment needs for NAS facilities.

1.1 OBJECTIVE.

The objective of this report is to provide the results of the evaluation to determine if the automated risk/vulnerability assessment tools previously surveyed comply with the components of the FAA's Security Analysis Framework for an automated risk/vulnerability assessment tool for NAS facilities.

1.2 BACKGROUND.

The automated tools evaluated in this report have been cataloged in the FAA Technical Center Technical Report, DOT/FAA/CT-94/48, Catalog of Automated Risk/Vulnerability Assessment Tools, July 1994. The catalog provides the general characteristics and features of the automated risk/vulnerability assessment tools. The 19 automated risk/vulnerability assessment tools evaluated in this report were also evaluated in the FAA Technical Center Technical Report, DOT/FAA/CT-94/50, Security Requirements Compliance Review: Automated Risk/Vulnerability Assessment Tools, September 1994, for compliance with FAA physical and computer security requirements.

1.3 SCOPE.

The evaluation was conducted only on those automated tools that were considered general purpose risk/vulnerability assessment tools in the previously prepared catalog. These automated risk/vulnerability assessment tools are evaluated against criteria derived from the Security Analysis Framework. This evaluation is not intended to be used as the sole source of data for the selection of an automated risk/vulnerability assessment tool for the FAA. Follow-up detailed user requirements analyses and in-depth, hands-on evaluation of the actual tools against these requirements needs to be conducted.

2. METHODOLOGY.

Each automated risk/vulnerability assessment tool was evaluated for its capability to comply with the criteria developed from the individual components of the Security Analysis Framework. The major components of the framework are as follows:

- a. Critical assets, risks, and threat likelihoods,

- b. Protection levels, system vulnerabilities, and impacts,
- c. Acceptable protection measure cost plus asset losses, and
- d. Cost-effective safeguard analysis and design.

Detailed components of the Security Analysis Framework are provided in Appendix A.

2.1 CRITERIA DEVELOPMENT.

The criteria developed from the Security Analysis Framework have been grouped into 4 major categories with a total of 16 subcategories. The categories and subcategories for the criteria are as follows:

- a. Security Threats,
 - 1) Threat types,
 - 2) Threat Characteristics,
 - 3) Threat Modes of Attack,
 - 4) Natural Threats,
 - 5) Design Threat Selection,
 - 6) Threat Likelihood Estimation,
- b. Critical Facility and Asset Identification,
 - 1) Facility Identification,
 - 2) Critical Asset Identification,
 - 3) Critical Asset Value,
- c. Protection Levels,
 - 1) Protection Level Calculation,
 - 2) Protection Level Selection,

- 3) Protection System Design Inputs,
- 4) Protection System Estimations,
- d. Cost-Effective Safeguards Analysis and Design,
 - 1) Basic Concepts,
 - 2) Generic Types of Real Time Security Systems, and
 - 3) Safeguard Evaluation.

A list of individual criterion for each subcategory are provided in Appendix C.

2.2 COMPLIANCE EVALUATION.

The evaluations of the automated risk/vulnerability assessment tools were conducted, where possible, using a hands-on approach with a version of the actual automated risk/vulnerability assessment tool. These automated tools were provided without cost by the sponsoring Government agency or commercial vendor. Where a complete and comprehensive demonstration version or limited version of the automated tool was available, it was used. In a few cases, it was not possible to obtain any version of the automated tool. In those cases the evaluation was based on claims made in comprehensive product literature provided by the tool supplier and interviews with supplier personnel. These claims were accepted as fact, but could not be validated or verified.

2.2.1 Evaluated Automated Tools.

The versions of the automated risk/vulnerability assessment tools that were used for this evaluation are as follows:

- a. Complete automated tool with documentation
 - (1) Analytic System and Software for Evaluating Safeguards and Security (ASSESS),
 - (2) Bayesian Decision Support System (BDSS),
 - (3) CCTA Risk Analysis and Management Methodology (CRAMM),
 - (4) Risk Assessment Matrix (RAM),

and

(5) Resource-Allocation Optimization Program for Safeguards (RAOPS),

(6) Security Assessment Model (SAM).

b. Abbreviated version of the automated tool with limited documentation

(1) Control-It,

(2) Expert Auditor/Probe Engine (EA/PE),

(3) Los Alamos Vulnerability Assessment (LAVA),

(4) Rank-It,

(5) RA/SYS, and

(6) RiskPac.

c. Marketing presentation/documentation only

(1) Buddy System,

(2) Criti-Calc,

(3) FRANTIC ABC,

(4) IRRAS,

(5) International Security Technology/Risk Analysis and Management Program (IST/RAMP),

(6) RiskMan, and

(7) RiskWatch.

2.2.2 Conditions of Compliancy.

Every automated tool was evaluated against each criterion to determine compliance with the Security Analysis Framework. For this evaluation, a tool was considered compliant if one of three conditions were met (or claims were made that they would be met):

a. The tool performed the process specified in the criterion,

- b. The tool used information or conditions specified in the criterion as input, or
- c. The tool provided information in the area specified by the criterion as output.

2.2.3 Compliance Ratings.

Each tool received one of the following four ratings for each criterion:

- a. Y - the tool meets the criterion,
- b. N - the tool does not meet the criterion and cannot be modified to meet it,
- c. M - the tool in the configuration supplied by the manufacturer does not meet the criterion, but can be modified by the user to meet it, or
- d. C - compliance could not be determined.

2.2.4 Evaluation Approach.

Each automated risk/vulnerability assessment tool was evaluated for compliance with the Security Analysis Framework criteria and provided ratings as cited in Section 2.2.3. The evaluations were made based on actual operation of the automated tool where possible, i.e., for ASSESS, BDSS, CRAMM, RAM, RAOPS, and SAM. Where the actual tool was not available (all others), the evaluations were made based on what was stated in the materials provided by the sponsoring Government agency or vendor. The claims of the sponsor or vendor in their materials could not be validated by this evaluation because the automated tool was not available.

3. COMPLIANCE EVALUATION FINDINGS.

This section provides the overall evaluation of each automated risk/vulnerability assessment tool for compliance with the requirements of the 16 criterion subcategories. A detailed breakdown of how the individual automated tool was rated against each criterion can be found in Appendix B.

3.1 ANALYTIC SYSTEM AND SOFTWARE FOR EVALUATING SAFEGUARDS AND SECURITY.

3.1.1 Description.

ASSESS is a scenario/simulation tool covering physical security of complex installations. It allows the definition of facilities, including their topology, occupants, and operating conditions. Based on this information, on internal data regarding vulnerability to intrusion, and on a model predicting the outcome of brief battles between guards and adversaries,

ASSESS pinpoints vulnerabilities, pinpoints the likeliest paths for attack, estimates the outcomes, and recommends safeguards. Modules include facility definition, neutralization, insider threat, outsider threat, and handoff/collusion (collaboration between insider and outsider agents).

3.1.2 Findings.

ASSESS performs threat assessments with a internal database of threat types, characteristics, and modes of attack. However, this database cannot be modified to factor in actual threat events that have occurred at the facility to determine threat likelihood. The ASSESS threat database also does not consider the severity levels of the different types of threats. ASSESS complies with the Critical Facility and Asset Identification criterion. ASSESS does not consider the operational, economic, or political consequences of a threat occurrence in calculating protection levels. Although ASSESS derives a recommended acceptable level of protection, it does not factor into its analysis the cost of providing the recommended protection level or existing facility budgets. ASSESS adequately addresses the different types of potential safeguards that could provide the recommended level of protection. However, in its evaluation of potential safeguards, it does not provide a cost comparison of what is achievable (e.g., within budget constraints) versus what is required.

3.2 BAYESIAN DECISION SUPPORT SYSTEM.

3.2.1 Description.

BDSS performs decision support and general risk/vulnerability assessment for information systems. It provides asset inventory/loss valuation, threat-vulnerability mapping, impact analysis, risk analysis, safeguard analysis, and cost-benefit analysis. It generates recommendations and what-if comparisons on safeguards. It includes a large database of threats and related safeguards. BDSS uses Bayesian Analysis to calculate the average annual loss exposure (AALE) and creates a wide variety of detailed and summary reports.

3.2.2 Findings.

BDSS evaluates threats in performing its risk/vulnerability assessments, but it does not factor in the different types of aggressors, tools or weapons used, or threat tactics. It also does not consider varying severity levels of the different types of threats. Historical local facility/surrounding area threat data can be factored into the BDSS threat assessment when modified by the system administrator. BDSS adequately meets the Critical Facility and Asset Identification criterion. BDSS provides a recommended acceptable level of protection and factors in safeguard costs into the analysis used to derive that recommendation. The BDSS safeguard recommendations are provided in a list that identifies them in general terms. BDSS does evaluate the cost effectiveness of the generic safeguards it recommends.

3.3 BUDDY SYSTEM.

3.3.1 Description.

The Buddy System provides risk/vulnerability assessment and safeguard selection for microcomputer or mainframe computer systems. It provides asset inventory/loss valuation, threat-vulnerability mapping, risk analysis, and safeguard analysis. The tool generates recommendations and what-if comparisons on safeguards. It includes a database of threats and related safeguards. It specifies mandatory safeguards. The system may be modified by the user to cover additional threats and safeguards within the questionnaire context.

3.3.2 Findings.

The Buddy System complies, or can be modified to comply, with most of the Security Analysis Framework criteria. It does not allow the user to input historical data on facility/surrounding area threat events to determine threat likelihood. The Buddy System does not factor in safeguard costs into its analysis to determine the design of the recommended protection system.

3.4 CONTROL-IT.

3.4.1 Description.

Control-It is a questionnaire-based risk analysis tool limited to controls on information systems. Control-It consists of four tools. Two tools teach users how to design and develop the control spreadsheet and how to rank the risks using the Delphi methodology. The main tool allows the user to design a control spreadsheet, identifying threats, ranking them, and selecting appropriate controls. The fourth tool allows attractive printing of graphics based on the control spreadsheet. Control-It includes databases of controls, threats, and system components. The user can add controls, but threats and safeguards that do not fit Control-It's basic layout and assumptions cannot be included. It does not cover physical security per se.

3.4.2 Findings.

Due to its ability to be modified, Control-It complies with most of the Security Analysis Framework criteria. However, Control-It has substantial limitations on the analyses it performs. Control-It does not analyze the likelihood of a threat occurring. Potential threats are provided in a list generated by its threat database for the user to select. A list of controls (safeguards) are also provided in a Control-It database. However, each recommended control is linked within Control-It to a single threat. Control-It performs no analysis to determine which control(s) best mitigate or eliminate a specific threat. These limitations significantly restrict the scope of the risk/vulnerability assessment that can be performed with this tool.

3.5 CCTA RISK ANALYSIS AND MANAGEMENT METHODOLOGY.

3.5.1 Description.

CRAMM is a risk analysis tool covering information system security. CRAMM provides asset valuation, threat/vulnerability assessment, and safeguard selection, with what-if capabilities. It works via user questionnaires.

3.5.2 Findings.

CRAMM performs all the basic elements of the Security Analysis Framework. However, the data used in its assessments cannot be modified to reflect threat likelihood based on facility historical threat data.

3.6 CRITI-CALC.

3.6.1 Description.

Criti-Calc is a microcomputer-based subset of IST/RAMP. It can be used for security planning, contingency planning, and risk analysis of information systems. It concentrates on information system security and covers physical security only as it relates to computer facilities. Criti-Calc uses a questionnaire to gather data on actual cost and frequency of computer service interruptions based on typical scenarios and causes of failure. It uses data familiar to end users to create and validate criticality ratings and threats.

3.6.2 Findings.

Criti-Calc meets many of the Security Analysis Framework criteria, however compliance with most of the other remaining criteria could not be determined without in-depth evaluation of the automated tool. In its threat analysis, Criti-Calc does not consider various aggressor types nor does it perform analyses based on historical threat data for the facility being assessed. Based on claims made in the Criti-Calc vendor literature, the tool evaluates the cost-effectiveness of the safeguards recommended for an acceptable level of protection.

3.7 EXPERT AUDITOR/PROBE ENGINE.

3.7.1 Description.

The Expert Auditor series administers automated security audits for 18 computer-related areas. The Probe Engine allows creation of new audits. Audit questionnaires use expert system rules to relate user's answers to given vulnerabilities. Expert Auditor creates a set of findings highlighting security problems and recommending specific controls. It does not include extensive databases, and covers physical security only as it relates to computer facility

security. Probe is a modifiable questionnaire-based risk tool, again covering mainly computer security.

3.7.2 Findings.

With its ability to modify the questionnaires used for data input, the Expert Auditor performs the basic elements of the Security Analysis Framework. Expert Auditor does not enable the user to factor in historical threat event data in analyzing threat likelihood. It can be modified to analyze and recommend physical security safeguards required by the framework.

3.8 FRANTIC ABC.

3.8.1 Description.

FRANTIC ABC is a time-dependent probabilistic risk assessment and reliability analysis of complex systems such as chemical or nuclear plants. It is an event tree-based system, based on user input and seven supplied model types, which calculates the probability at any given time that a system will react to an initiating event by moving into a safe state rather than failing with various catastrophic consequences. FRANTIC ABC allows what-if modeling of different events and components. Its functions do not include any threat, vulnerability, or safeguard databases, and it is not oriented toward physical security.

3.8.2 Findings.

FRANTIC ABC does not comply with the Security Threats and Countermeasure Analysis and Design elements of the Security Analysis Framework. FRANTIC ABC's ability to be modified, does enable it to fulfill some of the framework criteria. It does not address aggressor types nor does it allow the threat to be analyzed using actual local threat event data for the facility being assessed. In determining protection levels, FRANTIC ABC is not designed to consider existing budget constraints in deriving its recommended level of protection. The cost-benefit of individual safeguards is not factored into FRANTIC ABC's recommendations.

3.9 IRRAS.

3.9.1 Description.

IRRAS creates and analyzes fault/hazard trees, using graphical construction, cut set generation, and quantification. IRRAS is a tree-based system designed to conduct analyses of nuclear plants. Its functions do not include any threat, vulnerability, or safeguard databases, and it is not oriented toward physical security. It is supplied with event sets pertaining to nuclear facilities.

3.9.2 Findings.

Like its subset, FRANTIC ABC, IRRAS does not comply with the Security Threats and Countermeasure Analysis and Design elements of the Security Analysis Framework. IRRAS also has the ability to be modified so that it can fulfill some of the framework criterion. The findings for FRANTIC ABC related to the analysis of threats and determination of protection levels and recommended safeguards also apply to IRRAS.

3.10 INTERNATIONAL SECURITY TECHNOLOGY/RISK ANALYSIS AND MANAGEMENT PROGRAM.

3.10.1 Description.

IST/RAMP is a decision support and general risk management support tool for information systems. It is run on an IBM mainframe system running TSO or ROSCOE. Data entry is performed via a personal computer with the RAMP <> LINK feature. This feature enables user input to be used by the IST/RAMP program running on the mainframe system. IST/RAMP can produce disaster recovery guidance or plans. Its what-if capability helps the user select most effective safeguards.

3.10.2 Findings.

With the exception of a limited analysis of threats, IST/RAMP complies with most of the Security Analysis Framework criteria. Due to the lack of an actual version of IST/RAMP, compliance with many of the framework criteria could not be determined, especially criteria related to protection levels and safeguards. IST/RAMP will not accept facility actual threat event data input for consideration in its evaluation of threat likelihood. It also does not address aggressor types in its analysis of threats.

3.11 LOS ALAMOS VULNERABILITY ASSESSMENT.

3.11.1 Description.

LAVA is a multiple-module system with databases of threats, vulnerabilities, and safeguards in a number of areas including physical and information system security. It cannot be modified by the user. It is designed to conduct standard risk/vulnerability assessments, including calculation of Annual Loss Exposure (ALE).

3.11.2 Findings.

LAVA performs all the basic elements of the Security Analysis Framework. However, it does not comply with some threat and protection level criteria that are important to a risk/vulnerability assessment. For example, LAVA limits the user's ability to input threat data on events that have actually occurred at the facility being assessed. LAVA also does not

factor in the facility's budget when determining an acceptable level of protection or recommending safeguards.

3.12 RISK ASSESSMENT MATRIX.

3.12.1 Description.

RAM uses a questionnaire to obtain information about the occupants, contents, architecture, operating conditions, criminal history, and local threats of the facility under consideration. Using this information and internal data, RAM produces a graphical assessment of the potential risks to the facility and a matrix of recommended safeguards. A security specialist works with this matrix to provide cost information and to evaluate the recommendations. This information becomes a Cost Summary Document incorporating security planning data. RAM is not user-modifiable.

3.12.2 Findings.

RAM's analysis of the threat is limited in its compliance with the Security Analysis Framework. RAM does not consider the tactics, tools, or weapons used by an aggressor in its threat analysis. It also does not consider threat severity levels in its risk/vulnerability assessment. RAM does not provide the user a specified acceptable level of protection. The facility's budget is not given consideration by RAM in its determination of safeguards needed to provide the required level of protection. The risk/vulnerability assessment performed by RAM does not determine the operational, economic, or political consequences of a threat event occurring against a critical asset.

3.13 RANK-IT.

3.13.1 Description.

Rank-It is a limited-purpose tool designed to support a group of analysts in applying the Delphi method to determine the rankings of items such as threats and vulnerabilities. Its sole function is to allow users to list potential threats and vulnerabilities and to agree on their rank. Therefore, it can be modified to take any threat or vulnerability into account.

3.13.2 Findings.

Rank-It can be modified to comply on a limited scale with most of the Security Analysis Framework criteria. Rank-It does not allow the input of historical threat data or asset value data for use in its analyses. It also does not factor in facility budgets into the analysis performed for determining acceptable protection levels.

3.14 RESOURCE-ALLOCATION OPTIMIZATION PROGRAM FOR SAFEGUARDS.

3.14.1 Description.

RAOPS is an event tree-based tool designed to allocate security resources between guards and facility hardening. The user provides facility topography in tree form, attack scenarios, safeguards, and estimated likelihood of detection for each scenario, and total safeguard budget. It has no built-in databases of threats, vulnerabilities, or safeguards. Because the user can model any sequence of events, including the likelihood of a given threat overcoming a potential vulnerability, the tool can be modified to cover many of the types of safeguards listed in the criteria. However, it cannot model scenarios or safeguards that do not involve an active effort by a threat to exploit a vulnerability. Its program combines information to calculate cost-effective allocation of budget to safeguards.

3.14.2 Findings.

RAOPS does not factor in the identification and value of critical assets into its risk/vulnerability assessment. RAOPS can be modified to meet most of the other Security Analysis Framework criteria. Although RAOPS complies with most of the framework criteria for determining protection levels, it does not consider the operational, economic, and political consequences of the threat.

3.15 RA/SYS.

3.15.1 Description.

RA/SYS is a basic risk analysis system oriented toward information system security, with a limited list of built-in threats, vulnerabilities, and safeguards. RA/SYS performs asset valuation, threat lists, vulnerability lists, and safeguard lists. The user can add safeguards linked with threats or vulnerabilities. It calculates ALE and recommends safeguards from among those entered by the user. RA/SYS supports what-if analysis. However, it covers physical security only as directly related to computer facilities.

3.15.2 Findings.

RA/SYS complies with the Security Analysis Framework criteria, but on a limited scale. It does not have the capability to factor in threat likelihood based on actual historical threat data for the facility being assessed.

3.16 RISKMAN.

3.16.1 Description.

RiskMan is a scenario-based probabilistic risk assessment tool, using event sequence diagrams and fault tree analysis. It is intended for modeling complex systems, including system failure as well as external threats. It uses fault tree and event tree analysis to generate Probabilistic Risk Assessments according to Nuclear Regulation (NUREG) standards. RiskMan is not oriented specifically toward physical or computer security risk/vulnerability assessments. The user can construct event trees covering any series of events, but the tool has no database of threats, vulnerabilities, or safeguards.

3.16.2 Findings.

The ability of RiskMan to be modified enables it to comply with many of the Security Analysis Framework criteria. RiskMan's threat analysis process does not allow consideration of historical threat data for the facility being assessed. In determining the appropriate level of protection required, RiskMan does not factor in the facility's budget for additional or enhanced safeguards. RiskMan does not evaluate safeguards based on a cost-benefit basis nor on whether the safeguard is physically implementable for the facility being assessed.

3.17 RISKPAC.

3.17.1 Description.

RiskPac is a questionnaire-based system that performs standard risk/vulnerability assessments, security surveys, and operational audits for computer and information systems. It conducts asset inventory, threat-vulnerability mapping, risk analysis, safeguard analysis, and cost-benefit analysis. Questionnaires covering computer and physical security are included with the program. Users may create questionnaires relating to any set of threats, vulnerabilities, safeguards, and standards. RiskPac generates recommendations and what-if comparisons on safeguards. It includes a large database of threats and related standards, controls, and safeguards.

3.17.2 Findings.

RiskPac complies with most of the Security Analysis Framework criteria. It does not have the capability to perform threat analyses with historical threat data.

3.18 RISKWATCH.

3.18.1 Description.

RiskWatch is a completely modifiable system designed to cover security planning, risk analysis, and emergency and contingency plans. It supports computer and information system security, and is modifiable to cover any type of risk assessment. It performs asset inventory/loss valuation, threat-vulnerability mapping, impact analysis, risk analysis, safeguard analysis, cost-benefit analysis, and return on investment (ROI) assessments. It generates recommended security enhancements. RiskWatch contains a large database of threats and related safeguards in many categories, as well as threat frequency data. The database contains an exhaustive list of physical and information system threats, vulnerabilities and safeguards, and allows users to construct their own questionnaires covering additional areas. Question sets are available that include physical security, computer and telecommunications security, complex system or process risk, and more. RiskWatch allows what-if analysis.

3.18.2 Findings.

Based on its marketing literature, RiskWatch either complies or can be modified to comply with the Security Analysis Framework criteria. However, the modifications needed for compliance could be extensive and may not completely fulfill FAA's security requirements.

3.19 SECURITY ASSESSMENT MODEL.

3.19.1 Description.

SAM is a scenario/simulation tool covering physical security of complex installations. SAM allows users to define the facility, including its topography, construction materials, electronic security devices, guards, and surrounding roads. It has no provisions for covering information system issues except for the reachability of the installation by intruders. It cannot be used for contingency planning. It cannot model most types of safeguards. It performs superbly in modeling the design and hardening of facilities and the use of guard forces. Based on the analysis, SAM calculates threat likelihoods and intrusion success, then suggests cost-effective safeguards.

3.19.2 Findings.

SAM complies with most of the Security Analysis Framework criteria. Its only shortfall is that it does not address internal and natural threats in its threat analyses.

3.20 COMPOSITE FINDINGS.

Tables 1 and 2 provide a comparison of how well each automated risk/vulnerability assessment tool complies with the criteria in the 16 subcategories. Ratings are provided for

each automated tool as to whether the tool was compliant (Y), could be modified to be compliant (M), was non-compliant (N), or compliance could not be determined (C). The ratings in Tables 1 and 2 are based on the automated tool's ability to comply with the majority of the FAA criteria in the subcategories as indicated in Appendix B. In some subcategories the rating for a specific criterion/criteria was given precedence over the other criteria when providing the rating for that subcategory. The criterion/criteria given precedence are considered most important for fulfilling the appropriate framework element. Those criteria subcategories and the criterion having precedence are:

- a. Threat Characteristics - Aggressor Types,
- b. Threat Likelihood Estimation - Based on Historical Data,
- c. Protection Level Calculation - Likelihood of Threat Occurring,
- d. Protection Level Selection - Acceptable Level of Protection for Each Asset and Protection Level Consistent with the Value of the Asset,
- e. Protection System Design Inputs - Asset Identification and Value, and
- f. Countermeasure Evaluation - Most Cost-effective.

4. CONCLUSIONS.

Although many of the automated risk/vulnerability assessment tools comply with most of the Security Analysis Framework criteria, many of the ratings are derived from sponsoring agency or vendor claims made in marketing or other literature. Only 6 of the 19 automated tools were available for hands-on evaluation. Based on this limited evaluation, 10 of the automated risk/vulnerability assessment tools comply with most of the Security Analysis Framework criteria. Only 3 of these 10 automated tools were available in a complete version for evaluation (i.e., ASSESS, CRAMM, and SAM). The 10 automated risk/vulnerability assessment tools that met most of the framework criteria are:

- a. ASSESS,
- b. Buddy System,
- c. Control-It,
- d. CRAMM,
- e. Expert Auditor/Probe Engine,

Table 1. Comparison of Automated Risk/Vulnerability Assessment Tools

CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS								
	ASSESS	BDSS	Buddy System	Control-It	CRAMM	Criti-Calc	EA/PE	FRANTIC ABC	IRRAS
SECURITY THREATS									
Threat Types	Y	Y	Y	M	Y	Y	Y	M	M
Threat Characteristics	Y	N	M	M	N	N	M	N	N
Threat Modes of Attack	Y	N	M	Y	C	C	M	M	M
Natural Threats	Y	Y	Y	M	Y	Y	Y	M	M
Design Threat Selection	Y	Y	Y	Y	Y	Y	M	M	M
Threat Likelihood Estimation	N	N	N	N	N	N	N	N	N
CRITICAL FACILITY AND ASSET IDENTIFICATION									
Facility Identification	Y	Y	Y	M	Y	Y	Y	M	M
Critical Asset Identification	Y	Y	Y	Y	Y	Y	Y	M	M
Critical Asset Value	Y	Y	Y	M	Y	Y	M	M	M
PROTECTION LEVELS									
Protection Level Calculation	Y	Y	M	M	Y	Y	Y	Y	Y
Protection Level Selection	Y	Y	Y	M	C	C	Y	M	M
Protection System Design Inputs	Y	Y	Y	Y	Y	Y	Y	M	M
Protection System Estimations	N	N	M	M	C	C	M	N	N
COUNTERMEASURE ANALYSIS & DESIGN									
Basic Concepts	Y	N	M	M	C	C	M	M	M
Generic Types of Security Systems	Y	N	M	M	C	C	M	M	M
Countermeasure Evaluation	Y	Y	Y	Y	Y	Y	Y	N	N

Table 2. Comparison of Automated Risk/Vulnerability Assessment Tools (Continued)

CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
	IST/ RAMP	LAVA	RAM	Rank- It	RAOPS	RA/ SYS	RiskMan	RiskPac	RiskWatch	SAM
SECURITY THREATS										
Threat Types	Y	Y	Y	M	M	Y	M	Y	Y	Y
Threat Characteristics	N	Y	Y	M	Y	N	N	Y	Y	Y
Threat Modes of Attack	C	Y	N	M	Y	M	M	M	M	Y
Natural Threats	Y	Y	Y	M	M	Y	M	Y	Y	N
Design Threat Selection	Y	Y	Y	M	Y	Y	M	Y	Y	Y
Threat Likelihood Estimation	N	N	Y	N	N	N	N	N	Y	Y
CRITICAL FACILITY AND ASSET IDENTIFICATION										
Facility Identification	Y	Y	Y	M	N	Y	Y	Y	Y	Y
Critical Asset Identification	Y	Y	Y	M	N	Y	M	Y	Y	Y
Critical Asset Value	Y	Y	Y	M	Y	Y	Y	Y	Y	Y
PROTECTION LEVELS										
Protection Level Calculation	Y	Y	Y	M	Y	Y	Y	Y	Y	Y
Protection Level Selection	C	C	N	M	M	M	M	Y	Y	Y
Protection System Design Inputs	Y	Y	Y	N	Y	Y	M	Y	Y	Y
Protection System Estimations	C	Y	Y	N	Y	M	N	Y	Y	Y
COUNTERMEASURE ANALYSIS & DESIGN										
Basic Concepts	C	Y	N	M	Y	M	M	M	Y	Y
Generic Types of Security Systems	C	Y	Y	M	Y	Y	M	Y	Y	Y
Countermeasure Evaluation	Y	Y	Y	M	Y	M	N	Y	M	Y

- f. LAVA,
- g. RA/SYS,
- h. RiskPac,
- i. RiskWatch, and
- j. SAM.

The following sections discuss the applicability of each of these automated risk/vulnerability assessment tools complying with the FAA's Security Analysis Framework criteria.

4.1 ANALYTIC SYSTEM AND SOFTWARE FOR EVALUATING SAFEGUARDS AND SECURITY.

ASSESS is designed primarily to identify facility vulnerabilities. Although it performs the other elements of the Security Analysis Framework, it does not comply with several key framework criterion. ASSESS is oriented more to the protection of a facility than individual critical assets. ASSESS does not consider actual historical threat statistics nor threat severity levels in its analyses. Operational, economic, and political impacts are not considered in its analyses of the risk to the facility. ASSESS also does not collect the data required by a user for cost-benefit analyses of alternative safeguards.

4.2 BUDDY SYSTEM.

The Buddy System's ability to be modified enables it to comply with most of the Security Analysis Framework criteria. Like many of the tools, the Buddy System is not designed to factor into its analyses the actual quantitative threat data for the facility being assessed.

4.3 CONTROL-IT.

Control-It performs most of the Security Analysis Framework functions on a limited, non-quantitative basis. For example, Control-It's analysis of threats is limited to the small number of threat types included in the tool's database and does not allow the insertion or use of actual threat event statistical data.

4.4 CCTA RISK ANALYSIS AND MANAGEMENT METHODOLOGY.

CRAMM is another automated risk/vulnerability assessment tool that complies with most of the Security Analysis Framework criteria. However, CRAMM does not allow actual historical threat data to be considered in its analyses. CRAMM also does not have the capability to add other types of threats than what is contained in its database.

4.5 EXPERT AUDITOR/PROBE ENGINE.

Expert Auditor can be modified to comply with most of the Security Analysis Framework criteria. However, it does not allow the user to do a quantitative threat analysis using historical threat data for the facility.

4.6 LOS ALAMOS VULNERABILITY ASSESSMENT.

LAVA performs the major elements of the Security Analysis Framework, but with limited analyses in some areas. LAVA does not allow a quantitative threat analysis to be conducted using actual threat event statistics to determine threat likelihood. LAVA also does not consider existing and future facility and engineering budgets or safeguard costs in determining which safeguards it recommends for implementation.

4.7 RA/SYS.

RA/SYS complies with most of the Security Analysis Framework criteria with modifications that can be performed by the user. However, it also does not perform a quantitative threat analysis using actual facility threat data. Its limitations on the number of threats and safeguards that its databases can store may significantly restrict the scope of the risk/vulnerability assessment that can be conducted.

4.8 RISKPAC.

RiskPac complies with most of the Security Analysis Framework criteria with some modifications that can be made by the user. It also conducts threats analyses using only data that are embedded in its databases and will not allow more applicable local threat data to be applied.

4.9 RISKWATCH.

RiskWatch either currently complies or can be modified to comply with all of the Security Analysis Framework criteria based on claims made in the marketing literature used for this evaluation.

4.10 SECURITY ASSESSMENT MODEL.

SAM complies with most of the Security Analysis Framework criteria. However, SAM's threat analysis is limited as a result of its focus on external deliberate threats. SAM does not address internal or natural threats in its risk/vulnerability assessments.

5. RECOMMENDATION.

Since the evaluations of many of the automated risk/vulnerability assessment tools were made based solely on marketing materials and not the actual tool, it is recommended that FAA management select a limited number of automated tools for more detailed, hands-on evaluation prior to acquisition. The selection of automated tools for in-depth evaluation should be based on a detailed user requirements analysis and data provided in this report and the following reports:

- a. FAA Technical Center Technical Report, DOT/FAA/CT-94/48, Catalog of Automated Risk/Vulnerability Assessment Tools, July 1994,
- b. FAA Technical Center Technical Report, DOT/FAA/CT-94/49, Security Analysis Framework: National Airspace System (NAS) Facilities, Automated Risk/Vulnerability Assessment Tool, Volumes I-III, September 1994, and
- c. FAA Technical Center Technical Report, DOT/FAA/CT-94/50, Security Requirements Compliance Review: Automated Risk/Vulnerability Assessment Tools, September 1994.

6. REFERENCES.

The following references were used in the preparation of this report:

- a. FAA Technical Center Technical Report, DOT/FAA/CT-94/48, Catalog of Automated Risk/Vulnerability Assessment Tools, July 1994,
- b. FAA Technical Center Technical Report, DOT/FAA/CT-94/49, Security Analysis Framework: National Airspace System (NAS) Facilities, Automated Risk/Vulnerability Assessment Tool, Volumes I-III, September 1994,
- c. FAA Technical Center Technical Report, DOT/FAA/CT-94/50, Security Requirements Compliance Review: Automated Risk/Vulnerability Assessment Tools, September 1994,
- d. FAA Order 1600.6C, Physical Security Management Program, April 16, 1993,
- e. FAA Order 1810.1F, Acquisition Policy, March 10, 1993,
- f. Federal Information Processing Standards (FIPS) Publication (PUB) 102, Guideline for Computer Security Certification and Accreditation, National Institute of Standards and Technology, September 27, 1983,

g. Mendenhall, William, Introduction to Probability and Statistics, 6th Ed., Duxbury Press, Boston, 1983, and

h. FitzGerald, Ardra and FitzGerald, Jerry, Fundamentals of Systems Analysis, 3rd Ed., John Wiley and Sons, New York, 1987.

7. GLOSSARY.

Asset: The tangible and intangible resources of an entity. Tangible resources include items such as physical plant, hardware, software, data, cash, and personnel. Intangible resources include items such as good will. (FIPS PUB 102)

Bayesian Analysis: A method of incorporating the information from sample observations to adjust the probability of event. (Introduction to Probability and Statistics)

Cost/Benefit Analysis: An analysis undertaken to determine the relationship between life-cycle cost and the operational effectiveness of a concept or alternative that is technically feasible and can meet mission need. (FAA Order 1810.1F)

Countermeasure: A physical device, person, procedure, or combination of one or more of these intended to reduce or eliminate one or more identified vulnerabilities. (FAA Order 1600.6C)

Delphi Methodology: A data collection methodology where a small group of experts (three to seven) meet to develop a consensus in an area in which it may be impossible or too expensive to collect accurate data. (Fundamentals of Systems Analysis)

Physical Security: That part of security concerned with the implementation of physical measures designed to safeguard personnel to prevent unauthorized access to activities, property, equipment, and classified or sensitive unclassified information and to safeguard them against sabotage, espionage, fraud, waste and abuse, and other threats. (FAA Order 1600.6C)

Risk: A measure of the potential degree of loss of protected information. (FAA Order 1600.6C)

Risk Analysis: Method of quantifying the probability of loss or damage to an asset. (FAA Order 1600.6C)

Risk Assessment-Physical Assessment: Utilization of risk analysis techniques to identify level of physical security safeguards required for a facility, asset, or operation. (FAA Order 1600.6C)

Safeguard: See countermeasure.

Threat: The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operation. (FAA Order 1600.6C)

Vulnerability: Weakness in any aspect of an asset's design, use, mission, staffing, or other characteristic that if exploited would have an adverse impact on the security or operations of the asset. (FAA Order 1600.6C)

APPENDIX A - SECURITY ANALYSIS FRAMEWORK COMPONENTS

The following outline provides the components of the framework presented in the Federal Aviation Administration Technical Center Technical Report, DOT/FAA/CT-94/49 II, Security Analysis Framework: National Airspace System (NAS) Facilities, Automated Risk/Vulnerability Assessment Tool, Volume II (Technical Analysis), September 1994.

3. IDENTIFYING CRITICAL FACILITIES AND ASSETS

3.1 Identifying facility types and geographic locations

- ARTCCs, ATCTs

3.2 Identifying critical assets in each facility

3.2.1 Operationally critical assets, e.g., Host computer

3.2.2 High value assets, e.g., money, PCs

3.2.3 Personnel assets, e.g., critical to operations

4. ESTIMATING THREAT LIKELIHOODS

4.1 Threat Overview

4.1.1 Security Threats

4.1.1.1 Generic Security Threat Types

- Deliberate external "unauthorized" threats, e.g., criminals, vandals
- Deliberate internal "authorized" threats, e.g., employees, contractors, knowledgeable visitors

4.1.1.2 Security Threat Characteristics

- Aggressor objectives
 - Inflict injury or death on people
 - Destroy or damage facilities, equipment, or resources

- Steal equipment, material, or information
- Create adverse publicity
- Aggressor types
 - Criminals
 - Protestors
 - Terrorists
 - Vandals
 - Socio-psychopaths/disgruntled employees
 - Spies

4.1.1.3 Security Threat Modes of Attack

- Tools and weapons
 - Hand tools, e.g., hammer, hacksaw
 - Power tools, e.g., electric saw or drill
 - Thermal tools, e.g., cutting torch
 - Ballistic weapons, e.g., handguns, rifles
 - Explosives, e.g., TNT, plastic explosives
 - Incendiary devices, e.g., liquid flammables
 - Standoff Weapons, e.g., mortars
 - Contaminants, e.g., chemical agents
 - Surveillance devices, e.g., acoustical/visual
- Tactics
 - Forced entry
 - Covert entry
 - Insider compromise
 - Ballistics attack
 - Standoff weapons attack
 - Stationary bomb
 - Moving-vehicle bomb
 - Aircraft attack
 - Hand-thrown/placed
 - Surveillance compromise, i.e., obtaining sensitive information using acoustical/visual surveillance techniques and equipment
 - Chemical/biological contamination

- Radar jamming
- Communications interference
- Computer system compromise, i.e.,
disruption of operations (e.g., viruses)

4.1.2 Natural Threats

- Types
 - Tornadoes
 - Hurricanes
 - Earthquakes
 - Thunderstorms
 - Winter Storms
 - Volcanoes
 - Fires
 - Floods

4.1.3 Selecting the Design Threat

- Specific types of threat and their relative severity levels (e.g., low - very high)
- Concerned with broad range of possibilities over the life cycle of the facility (not prediction of immediate probability)
- Selection based upon assets being protected and their degree of vulnerability

4.2 Deliberate Security Threats

4.2.1 Potential application of expert judgements

4.2.2 User judgement

4.2.3 Estimating threat likelihoods based on historical precedent data (past attacks)

4.2.4 Estimating threat likelihood based on intelligence estimates (future attacks)

- Likelihood of a given aggressor being in the geographical area

- Aggressor's objective warrants the use of an attack at that severity level
- Aggressor has access to the required resources to carry through the attack

4.2.5 Deliberate threat data collection and analysis

- Historical data collection and analysis
- Intelligence data collection and analysis

4.3 Natural Threats

- Likelihood
 - History of threat occurring at the location
 - Analysis suggests threat may occur in the future

5. PROTECTION LEVELS, SYSTEM VULNERABILITIES, AND IMPACTS

5.1 Basic concepts

5.1.1 Calculating Protection Level and System Vulnerabilities

- Likelihood of a threat occurring
- Operational, economic, and political consequences of the threat

5.1.2 Vulnerabilities and Impacts

5.1.2.1 Vulnerabilities and expected economic loss impacts

- Replacement costs for damage to facility
- Replacement cost of asset
- Operation impact cost due to inoperable asset

5.1.2.2 Vulnerabilities and Operational Impacts

- For example, flight delays, passenger safety

5.1.2.3 Vulnerabilities and Political Impacts

- Visibility of asset, in the facility, at the location, to the public
- Asset perceived by the public as being important because of a high economic value
- Asset perceived by the public as being important because of a high operational value
- Asset perceived by the public as being important because of a high safety value

5.2 Framework for establishing acceptable levels of protection

5.2.1 Overview

5.2.2 AT output and its use in protection design

- Acceptable level of protection for each asset
- Maximum protection required over all assets contained in the facility

5.2.3 Acceptable protection level by FAA Order

- Protection level specified in FAA Order

5.2.4 Protection level consistent with the value of the asset

- Asset critical to operational readiness or safety
- Asset has a high economic worth
- There is a significant political impact if asset is stolen or destroyed

6. FRAMEWORK FOR ESTABLISHING ACCEPTABLE PROTECTION
MEASURE COST PLUS ASSET LOSSES

6.1 Appendix E framework results and its use in protection system design

- Inputs
 - Asset identification and value
 - Maximum construction budget for site preparation and protection related hardening of the building
 - Budget for such things as protection related sensor systems, guard personnel
 - Cost of acceptable level of asset losses over the life of the facility

6.2 Estimating budget limitations on protection measure costs

6.3 Estimating a maximum acceptable level of asset replacement costs

7. FRAMEWORK FOR COST-EFFECTIVE COUNTERMEASURE ANALYSIS
AND DESIGN

7.1 Basic concepts

7.1.1 Countermeasures to the security threat

7.1.1.1 Security system functional elements

- Deterring
- Detecting
- Assessing
- Delaying
- Protecting
- Responding

- 7.1.1.2 Real time security operating modes
 - Ingress denial (deny entry)
 - Egress denial (deny exit)
- 7.1.1.3 Security exclusion/containment zones
 - Perimeter zone, e.g., fenced area
 - Point zone, e.g., vault
- 7.1.1.4 Real time security performance timelines and spacial relationships
 - Detecting
 - Assessing
 - Delaying
 - Protecting
 - Responding
- 7.1.1.5 Generic types of real time security systems
 - Personnel intensive, e.g., guards
 - Systems with detection sensors, e.g., intrusion detection sensors (IDS)
 - Systems with detection sensors and assessment sensors, e.g., IDS, closed-circuit TVs (CCTV)
 - Systems with detection sensors, assessment sensors, delay, protection, and engagement hardware, e.g., IDS, (CCTV), cipher locks, vault doors

7.1.2 Protection against natural threats

7.1.2.1 Protection system functional elements

- Detecting (the occurrence)
- Assessing (the threat)
- Protecting (the asset from the effects of the threat)

7.1.2.2 Natural threat protection zones

- Building
- Halon fire protection zone

7.2 Analytical framework for countermeasure analysis and design

7.2.1 Procedure for selecting candidate protection countermeasures for evaluation

- Most cost-effective
- Provide acceptable level of protection

7.2.2 Countermeasure evaluation

7.2.2.1 Achievable versus required protection levels

- Equals or exceed an acceptable protection level for all assets within budgetary and other constraints

7.2.2.2 Countermeasures within budgetary cost constraints

- Total cost of CM to protect against all threats at facility; plus total expected losses summed of all assets for the level of protection achieved is less than or equal to some maximum level of loss plus costs

7.2.2.3 Protection measures are compatible with other constraints and requirements

- Political
- Regulatory
- Procedural or operational
- Facility or site-related

7.2.2.4 Protection level physically possible

(Following addresses determining probability weight factor)

7.2.2.5	Forced-entry attack
7.2.2.6	Covert entry
7.2.2.7	Firearms/ballistics
7.2.2.8	Standoff weapon attack
7.2.2.9	Moving ground vehicle bomb attack
7.2.2.10	Stationary bombs
7.2.2.11	Aircraft bomb attack
7.2.2.12	Hand-placed/thrown attacks
7.2.2.13	Eavesdropping
7.2.2.14	Airborne/waterborne contaminants
7.2.2.15	Deliberate internal threat
7.2.2.16	Communications interference
7.2.2.17	Computer system compromise
7.2.2.18	Radar jamming
7.2.2.19	Natural threats

APPENDIX B - AUTOMATED TOOL COMPLIANCE EVALUATION

This appendix provides the results of the evaluation of 19 automated risk/vulnerability assessment tools for compliance with Federal Aviation Administration Security Analysis Framework. The evaluation is recorded in two tables (Tables 3 and 4) due the large number of automated tools evaluated and the high number of criteria used. The criteria have been grouped into 4 categories and 16 subcategories for evaluation.

Each automated risk/vulnerability assessment tool has been rated for compliance with each criterion using the following:

- a. Y = the tool meets the criterion,
- b. N = the tool does not meet the criterion and cannot be modified to meet it,
- c. M = the tool in the configuration supplied by the manufacturer does not meet the criterion, but can be modified by the user to meet it, or
- d. C = compliance with the criterion could not be determined.

For this evaluation, a tool was considered compliant if one of three conditions were met (or claims were made that they would be met):

- a. The tool performed the process specified in the criterion,
- b. The tool used information or conditions specified in the criterion as input, or
- c. The tool provided information in the area specified by the criterion as output.

The compliance ratings for automated tools that were not available to the assessment team were derived based on claims made by the tool's sponsor/vendor in marketing literature and demonstration disks. For automated tools that were not available, the compliance has not be validated or verified.

Table 3. Automated Risk/Vulnerability Assessment Tool Evaluation

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS								
		ASSESS	BDSS	Buddy System	Control-It	CRAMM	Criti-Calc	Expert Auditor/Probe Engine	FRANTIC ABC	IRRAS
	CRITICAL FACILITY AND ASSET IDENTIFICATION									
3.1	Facility Identification									
	Type	Y	Y	Y	M	Y	Y	Y	M	M
	Geographical Location	Y	Y	Y	M	Y	Y	M	M	M
3.2	Critical Asset Identification									
	Operationally Critical Assets	Y	Y	Y	Y	Y	Y	Y	M	M
	High Value Assets	Y	Y	Y	Y	Y	Y	Y	M	M
	Personnel Assets	Y	Y	Y	Y	Y	Y	Y	M	M
5.1.2	Critical Asset Value									
	Critical to Operational Readiness or Safety	Y	Y	Y	M	Y	Y	M	M	M
	High Economic Worth	Y	Y	Y	M	Y	Y	Y	M	M
	Significant Political Impact if Stolen or Destroyed	Y	Y	Y	M	Y	C	M	M	M
	SECURITY THREATS									
4.1.1.1	Threat Types									
	Deliberate External	Y	Y	Y	M	Y	Y	Y	M	M
	Deliberate Internal	Y	Y	Y	M	Y	Y	Y	M	M

Table 3. Automated Risk/Vulnerability Assessment Tool Evaluation

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS								
		ASSESS	BDSS	Buddy System	Control- It	CRAMM	Critl- Calc	Expert Auditor/ Probe Engine	FRANTIC ABC	IRRAS
4.1.1.2	Threat Characteristics									
	Aggressor Objectives	Y	Y	M	M	Y	Y	M	M	M
	Aggressor Types	Y	N	M	M	N	N	M	N	N
4.1.1.3	Threat Modes of Attack									
	Tools and Weapons	Y	N	M	M	C	C	M	M	M
	Tactics	Y	N	M	Y	C	C	M	M	M
4.1.2	Natural Threats									
	Type	Y	Y	Y	M	Y	Y	Y	M	M
4.1.3	Design Threat Selection									
	Factors in Threat Severity Levels	N	C	C	M	Y	Y	M	M	M
	Considers Assets Being Protected	Y	Y	Y	Y	Y	Y	M	M	M
	Considers Vulnerability of Assets	Y	Y	Y	Y	Y	Y	M	M	M
4.2	Threat Likelihood Estimation									
	Based on Historical Data	N	N	N	N	N	N	N	N	N
	Based on Intelligence Estimates	Y	Y	Y	Y	Y	Y	Y	M	M

Table 3. Automated Risk/Vulnerability Assessment Tool Evaluation

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS								
		ASSESS	BDSS	Buddy System	Control-It	CRAMM	Criti-Calc	Expert Auditor/Probe Engine	FRANTIC ABC	IRRAS
	PROTECTION LEVELS									
5.1.1	Protection Level Calculation									
	Likelihood of Threat Occurring	Y	Y	M	M	Y	Y	Y	Y	Y
	Operational, Economic, and Political Consequences of Threat	N	Y	M	M	Y	Y	M	Y	Y
5.2	Protection Level Selection									
	Acceptable Level of Protection for Each Asset	Y	Y	Y	M	C	C	Y	M	M
	Maximum Protection Required for All Assets in the Facility	M	N	N	N	N	N	N	M	M
	Protection Level Specified by FAA	M	N	M	M	C	C	M	M	M
	Protection Level Consistent with the Value of the Asset	M	C	C	M	C	C	M	M	M
6.1	Protection System Design Inputs									
	Asset Identification and Value	Y	Y	Y	Y	Y	Y	Y	M	M
	Construction Budget for Site Preparation and Hardening	N	C	N	M	C	C	M	N	N
	Budget for Countermeasures Equipment/Personnel	N	C	N	M	C	C	M	N	N
	Cost of Acceptable Level of Asset Losses	N	C	M	M	Y	Y	M	N	N

Table 3. Automated Risk/Vulnerability Assessment Tool Evaluation

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS								
		ASSESS*	BDSS	Buddy System	Control- It	CRAMM	Criti- Calc	Expert Auditor/ Probe Engine	FRANTIC ABC	IRRAS
6.2, 6.3	Protection System Estimations									
	Budget Limitations	N	N	M	M	C	C	M	N	N
	Maximum Level of Asset Replacement Costs	N	N	M	M	C	C	M	N	N
	COST-EFFECTIVE COUNTERMEASURE ANALYSIS & DESIGN									
7.1.1	Basic Concepts									
	Security System Functional Elements	Y	N	M	M	C	C	M	M	M
	Real Time Security Operating Modes	Y	N	M	N	C	C	N	M	M
	Security Exclusion/Containment Zones	Y	N	M	M	C	C	M	M	M
	Real Time Security Performance Timelines	Y	N	M	N	C	C	N	M	M
	Generic Types of Real Time Security Systems	Y	N	M	M	C	C	M	N	N

Table 4. Automated Risk/Vulnerability Assessment Tool Evaluation (Continued)

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
		IST/ RAMP	LAVA	RAM	Rank- II	RAOPS	RA/ SYS	RiskMan	RiskPac	RiskWatch	SAM
3.1	CRITICAL FACILITY AND ASSET IDENTIFICATION										
	Facility Identification										
	Type	Y	Y	Y	M	N	Y	Y	Y	Y	Y
	Geographical Location	Y	Y	Y	M	N	Y	Y	Y	Y	Y
3.2	Critical Asset Identification										
	Operationally Critical Assets	Y	Y	Y	M	N	Y	M	Y	Y	Y
	High Value Assets	Y	Y	Y	M	N	Y	M	Y	Y	Y
	Personnel Assets	Y	Y	Y	M	N	Y	M	Y	Y	Y
5.1.2	Critical Asset Value										
	Critical to Operational Readiness or Safety	Y	Y	Y	M	Y	Y	Y	Y	Y	Y
	High Economic Value	Y	Y	Y	M	Y	Y	M	Y	Y	Y
	Significant Political Impact If Stolen or Destroyed	C	Y	Y	M	Y	N	M	Y	Y	Y
SECURITY THREATS											
	Threat Types										
	Deliberate External	Y	Y	Y	M	M	Y	M	Y	Y	Y
	Deliberate Internal	Y	Y	N	M	M	Y	M	Y	Y	N

Table 3. Automated Risk/Vulnerability Assessment Tool Evaluation

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
		ASSESS	BDSS	Buddy System	Control-It	CRAMM	Criti-Calc	Expert Auditor/Probe Engine	FRANTIC ABC	IRRAS	
7.1.1.5	Generic Types of Real Time Security Systems										
	Personnel Intensive	Y	N	M	M	C	C	M	M	M	
	Systems With Intrusion Detection Sensors (IDS)	Y	Y	M	M	C	C	M	M	M	
	Systems With IDS and Assessment Sensors	Y	N	M	M	C	C	M	M	M	
	Systems With IDS, Assessment Sensors, Delay, Protection and Engagement Hardware	Y	N	M	M	C	C	M	M	M	
	Countermeasure Evaluation										
	Most Cost-Effective	Y	Y	M	M	Y	Y	M	N	N	
	Provides Acceptable Level of Protection	Y	Y	Y	Y	Y	Y	Y	M	M	
	Achievable Versus Required Protection Levels	N	C	C	C	C	C	C	N	N	
	Countermeasures Within Budgetary Constraints	C	Y	C	C	C	C	C	N	N	
	Countermeasures are Compatible With Other Constraints and Requirements	C	Y	C	C	C	C	C	M	M	
	Protection Level Physically Possible	Y	C	C	C	C	C	C	N	N	

Table 4 contains the results of the evaluation of 10 additional automated tools.

Table 4. Automated Risk/Vulnerability Assessment Tool Evaluation (Continued)

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
		IST/ RAMP	LAVA	RAM	Rank- It	RAOPS	RA/ SYS	RiskMan	RiskPac	RiskWatch	SAM
4.1.1.2	Threat Characteristics										
	Aggressor Objectives	Y	Y	Y	M	Y	Y	M	Y	Y	Y
	Aggressor Types	N	Y	M	M	M	N	N	M	C	Y
4.1.1.3	Threat Modes of Attack										
	Tools and Weapons	C	Y	N	M	Y	M	M	M	M	Y
	Tactics	C	Y	N	M	M	M	M	M	M	Y
4.1.2	Natural Threats										
	Type	Y	Y	Y	M	M	Y	M	Y	Y	N
4.1.3	Design Threat Selection										
	Factors in Threat Severity Levels	Y	Y	N	M	Y	M	M	Y	Y	Y
	Considers Assets Being Protected	Y	Y	Y	M	Y	Y	M	Y	Y	Y
	Considers Vulnerability of Assets	Y	Y	Y	M	Y	Y	M	Y	Y	Y
4.2	Threat Likelihood Estimation										
	Based on Historical Data	N	N	Y	N	N	N	N	N	Y	Y
	Based on Intelligence Estimates	Y	Y	Y	Y	Y	Y	M	Y	Y	Y

Table 4. Automated Risk/Vulnerability Assessment Tool Evaluation (Continued)

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
		IST/ RAMP	LAVA	RAM	Rank- It	RAOPS	RA/ SYS	RiskMan	RiskPac	RiskWatch	SAM
	PROTECTION LEVELS										
5.1.1	Protection Level Calculation										
	Likelihood of Threat Occurring	Y	Y	Y	M	Y	Y	Y	Y	Y	Y
	Operational, Economic, and Political Consequences of Threat	Y	Y	N	M	N	Y	Y	Y	Y	Y
5.2	Protection Level Selection										
	Acceptable Level of Protection for Each Asset	C	Y	N	M	M	M	M	M	Y	Y
	Maximum Protection Required for All Assets in the Facility	N	N	N	M	M	N	M	N	M	C
	Protection Level Specified by FAA	C	N	N	M	M	M	M	M	M	C
	Protection Level Consistent with the Value of the Asset	C	C	Y	M	M	C	M	Y	M	Y
6.1	Protection System Design Inputs										
	Asset Identification and Value	Y	Y	Y	N	Y	Y	M	Y	Y	Y
	Construction Budget for Site Preparation and Hardening	C	N	Y	N	M	M	N	M	M	Y
	Budget for Countermeasures Equipment/Personnel	C	N	Y	N	Y	M	N	M	M	Y
	Cost of Acceptable Level of Asset Losses	Y	N	Y	N	Y	M	N	M	Y	Y

Table 4. Automated Risk/Vulnerability Assessment Tool Evaluation (Continued)

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
		IST/ RAMP	LAVA	RAM	Rank- It	RAOPS	RA/ SYS	RiskMan	RiskPac	RiskWatch	SAM
6.2, 6.3	Protection System Estimations										
	Budget Limitations	C	C	Y	N	Y	M	N	Y	M	Y
	Maximum Level of Asset Replacement Costs	C	Y	Y	N	M	M	N	M	Y	Y
	COST-EFFECTIVE COUNTERMEASURE ANALYSIS & DESIGN										
7.1.1	Basic Concepts										
	Security System Functional Elements	C	Y	N	M	Y	M	M	M	Y	Y
	Real Time Security Operating Modes	C	C	N	M	Y	M	M	M	M	Y
	Security Exclusion/Containment Zones	C	Y	Y	M	Y	M	M	M	M	Y
	Real Time Security Performance Timelines	C	C	N	M	Y	M	M	M	M	Y
	Generic Types of Real Time Security Systems	C	Y	Y	M	M	M	N	M	Y	Y

Table 4. Automated Risk/Vulnerability Assessment Tool Evaluation (Continued)

FRAMEWORK ELEMENT	CRITERIA	AUTOMATED RISK/VULNERABILITY ASSESSMENT TOOLS									
		IST/ RAMP	LAVA	RAM	Rank- It	RAOPS	RA/ SYS	RiskMan	RiskPac	RiskWatch	SAM
7.1.1.5	Generic Types of Real Time Security Systems										
	Personnel Intensive	C	Y	Y	M	Y	Y	M	Y	Y	Y
	Systems With Intrusion Detection Sensors (IDS)	C	Y	Y	M	Y	Y	M	Y	Y	Y
	Systems With IDS and Assessment Sensors	C	C	N	M	Y	M	M	M	M	Y
	Systems With IDS, Assessment Sensors, Delay, Protection and Engagement Hardware	C	C	N	M	Y	M	M	M	M	Y
7.2	Countermeasure Evaluation										
	Most Cost-Effective	Y	Y	Y	M	Y	M	N	Y	M	Y
	Provides Acceptable Level of Protection	Y	Y	Y	M	Y	Y	M	Y	Y	Y
	Achievable Versus Required Protection Levels	C	C	C	M	M	M	N	M	M	C
	Countermeasures Within Budgetary Constraints	C	C	Y	M	Y	M	N	M	M	Y
	Countermeasures are Compatible With Other Constraints and Requirements	C	C	C	M	N	M	M	M	Y	Y
	Protection Level Physically Possible	C	C	C	M	Y	M	N	M	M	Y

